SETS WITH FEW DIFFERENCES IN ABELIAN GROUPS

MITCHELL LEE

ABSTRACT. Let $(G, +)$ be an abelian group. In 2004, Eliahou and Kervaire found an explicit formula for the smallest possible cardinality of the sumset $A+A$, where $A \subseteq G$ has fixed cardinality r. We consider instead the smallest possible cardinality of the difference set $A - A$, which is always greater than or equal to the smallest possible cardinality of $A + A$ and can be strictly greater. We conjecture a formula for this quantity, and prove the conjecture in the case that G is a cyclic group or a vector space over a finite field. This resolves a conjecture of Bajnok and Matzke on signed sumsets.

1. INTRODUCTION

Let G be a finite abelian group of order N written with additive notation. Given subsets $A, B \subseteq G$, the *sumset* of A and B is defined as

$$A + B = \{a + b \mid a \in A, b \in B\}$$

and the *difference set* of A and B is defined as

$$A - B = \{a - b \mid a \in A, b \in B\}.$$

Let $-A$ denote the difference set $\{0\} - A = \{-a \mid a \in A\}$.

Given integers r and s with $1 \leq r, s \leq N$, define

$$\mu_G(r, s) = \min\{|A + B| \mid A, B \subseteq G, |A| = r, |B| = s\} \quad (1)$$

$$\rho_G^+(r) = \min\{|A + A| \mid A \subseteq G, |A| = r\} \quad (2)$$

$$\rho_G^-(r) = \min\{|A - A| \mid A \subseteq G, |A| = r\}. \quad (3)$$

We remark that taking $B = A$ in (1) yields $\mu_G(r, r) \leq \rho_G^+(r)$ and taking $B = -A$ yields $\mu_G(r, r) \leq \rho_G^-(r)$.

The functions $\mu_G(r, s)$ and $\rho_G^+(r)$ have held considerable interest for over 200 years. In 1813, Cauchy [4] proved the following classical result, which was rediscovered by Davenport [5] in 1935.

Theorem 1 (Cauchy-Davenport Theorem [4, 5]). *Let $G = \mathbb{Z}/p\mathbb{Z}$ where p is prime. Then $\mu_G(r, s) = \min\{r + s - 1, p\}$ for $1 \leq r, s \leq p$.*

In 2004, Eliahou and Kervaire [7] used a classical result of Kneser [8] to compute $\mu_G(r,s)$ and $\rho_G^+(r)$ for all finite abelian groups G.

Theorem 2 (Eliahou and Kervaire, [7, Theorem 2, Proposition 7])**.** *Let G be a finite abelian group of order N. Then*

$$\mu_G(r,s) = \min_{d \in D(N)} d\left(\left\lceil \frac{r}{d} \right\rceil + \left\lceil \frac{s}{d} \right\rceil - 1\right)$$

for $1 \leq r, s \leq N$, where $D(N)$ denotes the set of positive divisors of N. Furthermore, we have $\rho_G^+(r) = \mu_G(r,r)$.

Remark 1. By Theorem 2, the quantities $\mu_G(r,s)$ and $\rho_G^+(r)$ depend on N, r, and s, but not the group structure of G.

However, there is no known explicit formula for $\rho_G^-(r)$. In [1, 2], Bajnok and Matzke considered an h-fold variant of this problem. A small adaptation of their proofs yields the following upper bound for $\rho_G^-(r)$, which we conjecture holds with equality.

Theorem 3 (cf. [1, Theorem 5])**.** *Let G be a finite abelian group of order N. Let $e = \exp G$ be the exponent of G; that is, the least common multiple of the orders of the elements of G. For $1 \leq r \leq N$, define*

$$D(N,e,r) = \{d_1 d_2 \mid d_1 \in D(N/e), d_2 \in D(e), d_1 e \geq r\}.$$

Then

$$\rho_G^-(r) \leq \min_{d \in D(N,e,r)} d\left(2\left\lceil \frac{r}{d} \right\rceil - 1\right).$$

Conjecture 1 (cf. [1, Conjecture 10])**.** *The inequality in Theorem 3 holds with equality. That is, under the hypotheses of Theorem 3, we have*

$$\rho_G^-(r) = \min_{d \in D(N,e,r)} d\left(2\left\lceil \frac{r}{d} \right\rceil - 1\right).$$

Remark 2. We have the inequality $\rho_G^+(r) = \mu_G(r,r) \leq \rho_G^-(r)$, and it is possible that $\rho_G^+(r) < \rho_G^-(r)$. For example, if $G = (\mathbb{Z}/3\mathbb{Z})^2$, then $\rho_G^+(4) = 7$ and $\rho_G^-(4) = 9$. It is also worth noting that in contrast to $\rho_G^+(r)$ (see Remark 1), the quantity $\rho_G^-(r)$ cannot be determined from N and r alone.

The goal of this paper is to prove two important special cases of Conjecture 1.

First, consider the case that $G = \mathbb{Z}/N\mathbb{Z}$ is a finite cyclic group. In this case, we have $e = \exp G = N$, so $D(N,e,r) = D(N)$ for $1 \leq r \leq N$. Thus, the statement of Conjecture 1 becomes Theorem 4 below.

Theorem 4 (cf. [1, Theorem 4]). *Let $G = \mathbb{Z}/N\mathbb{Z}$. Then*

$$\rho_G^-(r) = \min_{d \in D(N)} d\left(2\left\lceil \frac{r}{d} \right\rceil - 1\right)$$

for $1 \le r \le N$.

Second, consider the case that $G = (\mathbb{Z}/p\mathbb{Z})^d$ where p is prime and $d \ge 0$. Then Theorem 5 below, which is the main result of this paper, computes $\rho_G^-(r)$ for $1 \le r \le p^d$. We will verify in Section 4 that Theorem 5 agrees with the prediction given by Conjecture 1.

Theorem 5. *Let $G = (\mathbb{Z}/p\mathbb{Z})^d$ where p is prime and $d \ge 0$. Let t and r be integers with $0 \le t \le d$ and $p^t < r \le p^{t+1}$. Then*

$$\rho_G^-(r) = p^t \min\left\{2\left\lceil \frac{r}{p^t} \right\rceil - 1, p\right\}.$$

As a consequence of Theorem 5, we obtain the following result, which appears as Conjecture 18 in [2]. We use the notation $\rho_\pm(G, m, r)$ defined in [2].

Theorem 6 ([2, Conjecture 18]). *Let $p > 2$ be a prime number, and let c and v be integers with $0 \le c \le p-1$ and $1 \le v \le p$. Let $m = cp + v$.*
(a) If $1 \le c \le (p-3)/2$, then

$$\rho_\pm((\mathbb{Z}/p\mathbb{Z})^2, m, 2) = (2c+1)p.$$

(b) If $c = (p-1)/2$ and $v \le (p-1)/2$, then

$$\rho_\pm((\mathbb{Z}/p\mathbb{Z})^2, m, 2) = p^2 - 1.$$

In Section 2, we will prove Theorem 4. In Section 3, we will prove Theorem 3. In Sections 4 to 7, we will prove Theorem 5. Finally, in Section 8, we will prove Theorem 6.

2. The cyclic case

The goal of this section is to prove Theorem 4, which computes $\rho_G^-(r)$ in the case that G is a finite cyclic group. The proof closely follows that of [1, Theorem 4], though it should be noted that Theorem 4 does not follow directly from [1, Theorem 4] due to differences in the definitions of $2_\pm A$ and $A - A$.

Theorem 4 (cf. [1, Theorem 4]). *Let $G = \mathbb{Z}/N\mathbb{Z}$. Then*

$$\rho_G^-(r) = \min_{d \in D(N)} d\left(2\left\lceil \frac{r}{d} \right\rceil - 1\right)$$

for $1 \le r \le N$.

Proof of Theorem 4. By Theorem 2, we have

$$\rho_G^-(r) \geq \mu_G(r,r) = \min_{d \in D(N)} d\left(2\left\lceil \frac{r}{d} \right\rceil - 1\right)$$

so it remains to show that

$$\rho_G^-(r) \leq \min_{d \in D(N)} d\left(2\left\lceil \frac{r}{d} \right\rceil - 1\right).$$

It suffices to show that

$$\rho_G^-(r) \leq d\left(2\left\lceil \frac{r}{d} \right\rceil - 1\right)$$

for each $d \in D(N)$. For this, we will construct a set $A \subseteq G$ with $|A| \geq r$ and

$$|A - A| \leq d\left(2\left\lceil \frac{r}{d} \right\rceil - 1\right).$$

Let H be the subgroup of G of order d, and let x be a generator for G/H. Take A to be the "coset arithmetic progression"

$$A = \bigcup_{i=0}^{\lceil r/d \rceil - 1} (H + ix).$$

We compute

$$A - A = \bigcup_{i=1-\lceil r/d \rceil}^{\lceil r/d \rceil - 1} (H + ix),$$

so $|A| = d\lceil r/d \rceil \geq r$ and

$$|A - A| \leq d\left(2\left\lceil \frac{r}{d} \right\rceil - 1\right)$$

as desired. □

Remark 3. By comparing the expressions in Theorem 2 and Theorem 4, we see that $\rho_G^-(r) = \rho_G^+(r) = \mu_G(r,r)$ for $1 \leq r \leq N$ if $G = \mathbb{Z}/N\mathbb{Z}$ is a finite cyclic group.

3. An upper bound on $\rho_G^-(r)$

We shall now restate and prove Theorem 3. The proof very closely follows that of [1, Theorem 5].

Theorem 3 (cf. [1, Theorem 5])**.** *Let G be a finite abelian group of order N. Let $e = \exp G$ be the exponent of G; that is, the least common multiple of the orders of the elements of G. For $1 \leq r \leq N$, define*

$$D(N,e,r) = \{d_1 d_2 \mid d_1 \in D(N/e), d_2 \in D(e), d_1 e \geq r\}.$$

Then

$$\rho_G^-(r) \leq \min_{d \in D(N,e,r)} d\left(2\left\lceil \frac{r}{d} \right\rceil - 1\right).$$

Proof. It suffices to show that

$$\rho_G^-(r) \leq d\left(2\left\lceil \frac{r}{d} \right\rceil - 1\right)$$

for each $d \in D(N,e,r)$. For this, we will construct a set $A \subseteq G$ with $|A| \geq r$ and

$$|A - A| \leq d\left(2\left\lceil \frac{r}{d} \right\rceil - 1\right).$$

Write $d = d_1 d_2$ for $d_1 \in D(N/e)$, $d_2 \in D(e)$, and $d_1 e \geq r$.

By the structure theorem for finitely generated abelian groups, the group G is isomorphic to a direct product $H \times (\mathbb{Z}/e\mathbb{Z})$ for some abelian group H with $|H| = N/e$. Since $d_1 \in D(N/e)$, we can find a subgroup $A_1 \subseteq H$ with $|A_1| = d_1$. Let $s = \lceil r/d_1 \rceil$. Then $s \leq e$, so by Theorem 4 there is a subset $A_2 \subseteq \mathbb{Z}/e\mathbb{Z}$ with $|A_2| = s$ and

$$|A_2 - A_2| \leq d_2\left(2\left\lceil \frac{s}{d_2} \right\rceil - 1\right).$$

Take $A = A_1 \times A_2 \subseteq H \times (\mathbb{Z}/e\mathbb{Z}) \cong G$. Then $|A| = d_1 s = d_1 \lceil r/d_1 \rceil \geq r$ and

$$\begin{aligned}
|A - A| &= |(A_1 \times A_2) - (A_1 \times A_2)| \\
&= |(A_1 - A_1) \times (A_2 - A_2)| \\
&= |A_1 - A_1||A_2 - A_2| \\
&\leq d_1\left(d_2\left(2\left\lceil \frac{\lceil r/d_1 \rceil}{d_2} \right\rceil - 1\right)\right) \\
&= d\left(2\left\lceil \frac{r}{d} \right\rceil - 1\right)
\end{aligned}$$

as desired. □

4. An outline of the proof of Theorem 5

Sections 4 to 7 of this paper will contain the proof of Theorem 5, which will proceed in four steps:

(1) We will show that the bound given in Theorem 5 is achieved. That is, we will show that

$$\rho_G^-(r) \leq p^t \min\left\{2\left\lceil \frac{r}{p^t} \right\rceil - 1, p\right\}.$$

(2) We will show that for $G = (\mathbb{Z}/p\mathbb{Z})^d$, the quantity $\rho_G^-(r)$ only depends on r and p and not d, as long as d is large enough that $\rho_G^-(r)$ is defined (that is, $r \leq p^d$).
(3) By applying the Cauchy-Davenport Theorem (Theorem 1) repeatedly, we will prove Theorem 5 in the case that $r \leq p^2$.
(4) We will conclude the proof of the theorem by induction on r.

We start with the following result, which is step (1) above.

Lemma 1. *With the notation of Theorem 5, we have*

$$\rho_G^-(r) \leq p^t \min\left\{2\left\lceil \frac{r}{p^t}\right\rceil - 1, p\right\}.$$

Proof. Using the notation of Theorem 3, we have $N = |G| = p^d$ and $e = \exp G = p$, so

$$\begin{aligned} D(N, e, r) &= \{d_1 d_2 \mid d_1 \in D(p^{d-1}), d_2 \in D(p), d_1 p \geq r\} \\ &= \{p^t, p^{t+1}, \ldots, p^{d-1}, p^d\}. \end{aligned}$$

By Theorem 3, we have

$$\begin{aligned} \min_{d \in D(N,e,r)} d\left(2\left\lceil \frac{r}{d}\right\rceil - 1\right) &= \min\left\{p^t\left(2\left\lceil \frac{r}{p^t}\right\rceil - 1\right), p^{t+1}, \ldots, p^{d-1}, p^d\right\} \\ &= p^t \min\left\{2\left\lceil \frac{r}{p^t}\right\rceil - 1, p\right\}, \end{aligned}$$

as desired. □

Remark 4. The proof of Lemma 1 given above shows that Theorem 5 agrees with the prediction given by Conjecture 1.

Remark 5. Here is an explicit example of a subset $A \subseteq G$ achieving the bound of Lemma 1. Put a total order $<$ on $\mathbb{Z}/p\mathbb{Z}$ by identifying it with $\{0, 1, \ldots, p-1\}$ in the usual way. Then, recall that $(\mathbb{Z}/p\mathbb{Z})^d$ is totally ordered by the *lexicographic order*, which is defined as follows: we say that $x = (x_1, \ldots, x_d)$ precedes $y = (y_1, \ldots, y_d)$ in the lexicographic order if for some i we have $x_i < y_i$ and $x_j = y_j$ for $j < i$. Let A be the set of the smallest r elements of $(\mathbb{Z}/p\mathbb{Z})^d$ in the lexicographic order. Then one can easily verify that

$$|A - A| = p^t \min\left\{2\left\lceil \frac{r}{p^t}\right\rceil - 1, p\right\},$$

which provides an alternative constructive proof of Lemma 1. It is worth noting that by [6, Proposition 3.1], the same set A satisfies $|A + A| = \rho_G^+(r)$.

5. Independence of dimension

The following result is step (2) in the proof of Theorem 5.

Lemma 2. *Let p be a prime and let $d_1 > d_2 \geq 0$ be integers. Let $G = (\mathbb{Z}/p\mathbb{Z})^{d_1}$ and $H = (\mathbb{Z}/p\mathbb{Z})^{d_2}$. Then $\rho_G^-(r) = \rho_H^-(r)$ for $1 \leq r \leq p^{d_2}$.*

Proof. It suffices to consider the case that $d_1 = d_2 + 1$. Since H embeds in G as a subgroup, we have $\rho_G^-(r) \leq \rho_H^-(r)$, so it remains to show that $\rho_H^-(r) \leq \rho_G^-(r)$.

Take a subset $A \subseteq G$ with $|A| = r$ and $|A - A| = \rho_G^-(r)$. Considering G as a vector space of dimension $d_1 = d_2 + 1$ over the finite field $\mathbb{F}_p$, there are

$$\frac{p^{d_1} - 1}{p - 1} = 1 + p + \cdots + p^{d_2} \geq p^{d_2}$$

lines containing 0 (that is, vector subspaces of dimension 1) in G. On the other hand, there are only

$$|A - A| - 1 \leq \rho_G^-(r) - 1 \leq \rho_H^-(r) - 1 < p^{d_2}$$

nonzero elements of $A - A$. Since no two distinct lines in G containing 0 share a nonzero element, we conclude that there is a line ℓ in G such that $\ell \cap (A - A) = \{0\}$.

Considering H as a vector space of dimension $d_2 = d_1 - 1$ over $\mathbb{F}_p$, fix an $\mathbb{F}_p$-linear transformation $\pi : G \to H$ whose kernel is the line ℓ. Such a transformation π exists because

$$\dim_{\mathbb{F}_p} \ell + \dim_{\mathbb{F}_p} H = 1 + d_2 = d_1 = \dim_{\mathbb{F}_p} G.$$

We claim that the restriction $\pi|_A$ is an injection. To show this, take $x, y \in A$ with $\pi(x) = \pi(y)$; we will show that $x = y$. Since π is linear, we have $\pi(x - y) = 0$, so $x - y \in \ker \pi = \ell$. Therefore, we have $x - y \in \ell \cap (A - A) = \{0\}$. That is, we have $x = y$, as desired.

Since $\pi|_A$ is an injection, we have $|\pi(A)| = |A| = r$, where $\pi(A)$ is the image of A under the map π. Therefore

$$\rho_H^-(r) \leq |\pi(A) - \pi(A)| = |\pi(A - A)| \leq |A - A| = \rho_G^-(r)$$

as desired. $\square$

6. The case $r \leq p^2$

In this section, we show that the statement of Theorem 5 holds when $r \leq p^2$, which is step (3) in the proof of Theorem 5.

Lemma 3. *Let p be a prime and let d be a nonnegative integer. Let G be the group $(\mathbb{Z}/p\mathbb{Z})^d$. Then*

$$\rho_G^-(r) = p^t \min\left\{2\left\lceil \frac{r}{p^t}\right\rceil - 1, p\right\}$$

for $1 \leq r \leq \min\{p^d, p^2\}$, where t is the unique integer satisfying $p^t < r \leq p^{t+1}$.

The following lemma will be instrumental in the proof of Lemma 3.

Lemma 4. *Let p be a prime, and let m and n be integers with $n \geq 1$ and $n + 2 \leq m \leq (p-1)/2$. Let $\lambda = (\lambda_1, \ldots, \lambda_m)$ be a sequence of integers with $p \geq \lambda_1 \geq \cdots \geq \lambda_m > 0$ and $\sum_{k=1}^m \lambda_k \geq np + 1$. Let $\mu = (\mu_1, \ldots, \mu_{2m-1})$ be a sequence of integers such that $\mu_{i+j-1} \geq \min\{\lambda_i + \lambda_j - 1, p\}$ for $1 \leq i, j \leq m$. Then*

$$\sum_{k=1}^{2m-1} \mu_k \geq (2n+1)p.$$

Proof. We defer the proof to Appendix A. □

Proof of Lemma 3. By Lemma 1, we have

$$\rho_G^-(r) \leq p^t \min\left\{2\left\lceil \frac{r}{p^t}\right\rceil - 1, p\right\},$$

so it remains to show that

$$\rho_G^-(r) \geq p^t \min\left\{2\left\lceil \frac{r}{p^t}\right\rceil - 1, p\right\}. \tag{4}$$

If $r \leq p$, then this follows directly from Lemma 2 and the Cauchy-Davenport Theorem. Thus, we may assume $r > p$.

By Lemma 2, we may assume that $d = 2$, so $G = (\mathbb{Z}/p\mathbb{Z})^2$. If $p = 2$, then the theorem follows easily from enumerating all possible values of r and all sets $A \subseteq G$, so assume that $p > 2$. Let

$$r' = \begin{cases} p\left(\lceil r/p\rceil - 1\right) + 1 & \text{if } r \leq p(p-1)/2 \\ p(p-1)/2 + 1 & \text{if } r > p(p-1)/2 \end{cases}.$$

Since $r \geq r'$, replacing r with r' cannot increase the left-hand side of (4), and it is easy to check that this replacement leaves the right-hand side unchanged. Therefore, we may assume that $r = np + 1$ where $1 \leq n \leq (p-1)/2$. Take a subset $A \subset G$ with $|A| = r$; we will show that

$$|A - A| \geq (2n+1)p = p^t \min\left\{2\left\lceil \frac{r}{p^t}\right\rceil - 1, p\right\}.$$

Identify G with the two-dimensional vector space $\mathbb{F}_p^2$ over the field $\mathbb{F}_p$. We will now count the two-element subsets of A in two ways. By definition, the number of two-element subsets of A is the binomial coefficient $\binom{np+1}{2}$. On the other hand, every two-element subset of A is contained in a unique line (that is, affine subspace of G of dimension 1), so we can count these subsets according to the lines containing them. This yields

$$\sum_{\ell \subset G} \binom{|A \cap \ell|}{2} = \binom{np+1}{2} \tag{5}$$

where the sum is over all lines $\ell \subset G$. Every line in G is parallel to exactly one line $\ell' \subset G$ containing 0, so (5) can be rewritten as

$$\sum_{\substack{\ell' \subset G \\ \ell' \ni 0}} \sum_{\substack{\ell \subset G \\ \ell \| \ell'}} \binom{|A \cap \ell|}{2} = \binom{np+1}{2}$$

where the outer sum is over all lines $\ell' \subset G$ containing 0, and the inner sum is over all lines $\ell \subset G$ parallel to ℓ'. Since there are exactly $p+1$ lines in G containing 0, there is a particular line $\ell_0 \subset G$ containing 0 such that

$$\sum_{\substack{\ell \subset G \\ \ell \| \ell_0}} \binom{|A \cap \ell|}{2} \geq \frac{1}{p+1} \binom{np+1}{2}.$$

We may assume, by applying an $\mathbb{F}_p$-linear change of coordinates, that ℓ_0 is the line $\{(0, y) \mid y \in \mathbb{F}_p\} \subset \mathbb{F}_p^2 = G$. For any $x \in \mathbb{F}_p$, define the line

$$\ell_x = \{(x, y) \mid y \in \mathbb{F}_p\}.$$

Then, the lines in G parallel to ℓ_0 are exactly the lines ℓ_x for $x \in \mathbb{F}_p$. Let

$$m = \max_{x \in \mathbb{F}_p} |A \cap \ell_x|.$$

Since

$$\sum_{x \in \mathbb{F}_p} |A \cap \ell_x| = |A| = np + 1,$$

we have $m \geq \lceil (np+1)/p \rceil = n+1$. We consider three cases, depending on whether $m \geq (p+1)/2$, or $m = n+1$, or $n+2 \leq m \leq (p-1)/2$.

Case 1 ($m \geq (p+1)/2$)**:**
Take $x \in \mathbb{F}_p$ such that $|A \cap \ell_x| = m$. Since ℓ_x is a translate of ℓ_0, which is isomorphic as a group to $\mathbb{Z}/p\mathbb{Z}$, the Cauchy-Davenport Theorem applies to the difference $(A \cap \ell_x) - (A \cap \ell_x) \subseteq \ell_0$, yielding

$$|(A - A) \cap \ell_0| \geq |(A \cap \ell_x) - (A \cap \ell_x)| \geq \min\{2m - 1, p\} = p.$$

(Essentially, we are applying the Cauchy-Davenport Theorem only to the second coordinates of the elements of $A \cap \ell_x$, which lie in $\mathbb{Z}/p\mathbb{Z}$.) That is, the line ℓ_0 is a subset of $A - A$.

Now, take *any* line $\ell' \subset G$ containing 0. There is a line ℓ parallel to ℓ' such that $|A \cap \ell| \geq \lceil (np+1)/p \rceil = n+1$. Since ℓ is a translate of ℓ', which is isomorphic as a group to $\mathbb{Z}/p\mathbb{Z}$, the Cauchy-Davenport Theorem again applies to the difference $(A \cap \ell) - (A \cap \ell) \subseteq \ell'$, yielding

$$|(A - A) \cap \ell'| \geq |(A \cap \ell) - (A \cap \ell)| \geq \min\{2(n+1) - 1, p\} = 2n + 1.$$

Since $G \setminus \{0\}$ is equal to the disjoint union

$$\bigsqcup_{\substack{\ell' \subset G \\ \ell' \ni 0}} (\ell' \setminus \{0\})$$

over all lines $\ell' \subset G$ containing 0, we conclude

$$\begin{aligned}
|A - A| &= 1 + \sum_{\substack{\ell' \subset G \\ \ell' \ni 0}} (|(A - A) \cap \ell'| - 1) \\
&\geq 1 + (p - 1) + p \cdot ((2n + 1) - 1) \\
&= (2n + 1)p
\end{aligned}$$

which is the desired inequality.

Case 2 $(m = n + 1)$**:**
Let $S = \{x \in \mathbb{F}_p \mid |A \cap \ell_x| = n+1\}$ and let $s = |S|$. For each $x \in \mathbb{F}_p \setminus S$ we have $|A \cap \ell_x| \leq n$, so

$$\begin{aligned}
\frac{1}{p+1}\binom{np+1}{2} &\leq \sum_{x \in \mathbb{F}_p} \binom{|A \cap \ell_x|}{2} \\
&= s\binom{n+1}{2} + \sum_{x \in \mathbb{F}_p \setminus S} \binom{|A \cap \ell_x|}{2} \\
&\leq s\binom{n+1}{2} + \sum_{x \in \mathbb{F}_p \setminus S} \frac{n-1}{2} |A \cap \ell_x| \\
&= s\binom{n+1}{2} + \frac{n-1}{2}((np + 1) - (n + 1)s),
\end{aligned}$$

Simplifying this inequality and using the bound $n \le (p-1)/2$, we obtain

$$\begin{aligned} s &\ge \frac{p+1-n}{p+1} \cdot \frac{np+1}{n+1} \\ &\ge \frac{p+1-(p-1)/2}{p+1} \cdot \frac{p(p-1)/2+1}{(p-1)/2+1} \\ &= \frac{p-1}{2} + \frac{p^2+7}{2(p+1)^2} \\ &> \frac{p-1}{2}. \end{aligned}$$

Thus $s \ge (p+1)/2$, so by the Cauchy-Davenport Theorem, we have $|S-S| \ge \min\{2s-1, p\} = p$, so $S - S = \mathbb{F}_p$.

Now, take any $x \in \mathbb{F}_p$. Since $x \in S - S$, there is $y \in \mathbb{F}_p$ such that $y, x+y \in S$. By the Cauchy-Davenport Theorem again, we have

$$|(A-A) \cap \ell_x| \ge |A \cap \ell_{x+y} - A \cap \ell_y| \ge \min\{2(n+1)-1, p\} = 2n+1.$$

Summing over all $x \in \mathbb{F}_p$ yields

$$|A-A| = \sum_{x \in \mathbb{F}_p} |(A-A) \cap \ell_x| \ge (2n+1)p$$

as desired.

Case 3 $(n+2 \le m \le (p-1)/2)$**:**
For $1 \le k \le p$, define

$$\begin{aligned} \Lambda_k &= \{x \in \mathbb{F}_p \mid |A \cap \ell_x| \ge k\} \\ M_k &= \{x \in \mathbb{F}_p \mid |(A-A) \cap \ell_x| \ge k\} \\ \lambda_k &= |\Lambda_k| \\ \mu_k &= |M_k| \end{aligned}$$

By definition, we have $p \ge \lambda_1 \ge \cdots \ge \lambda_m > 0$ and $p \ge \mu_1 \ge \cdots \ge \mu_p \ge 0$. We have

$$\sum_{k=1}^{m} \lambda_k = \sum_{x \in \mathbb{F}_p} |A \cap \ell_x| = |A| = ap + 1$$

because each line ℓ_x contributes exactly $|A \cap \ell_x|$ to the sum. Similarly

$$\sum_{k=1}^{p} \mu_k = \sum_{x \in \mathbb{F}_p} |(A-A) \cap \ell_x| = |A-A|.$$

We claim that $M_{i+j-1} \supseteq \Lambda_i - \Lambda_j$ for $1 \leq i, j \leq m$. To show this, take $x_1 \in \Lambda_i$ and $x_2 \in \Lambda_j$; we will show that $x_1 - x_2 \in M_{i+j-1}$. By the Cauchy-Davenport Theorem, we have

$$\begin{aligned} |(A - A) \cap \ell_{x_1 - x_2}| &\geq |A \cap \ell_{x_1} - A \cap \ell_{x_2}| \\ &\geq \min\{|A \cap \ell_{x_1}| + |A \cap \ell_{x_2}| - 1, p\} \\ &\geq \min\{i + j - 1, p\} \\ &= i + j - 1 \end{aligned}$$

where the last equality follows from the bound $i, j \leq m \leq (p-1)/2$. That is, we have $x_1 - x_2 \in M_{i+j-1}$, as desired.

By the Cauchy-Davenport Theorem again, we conclude

$$\mu_{i+j-1} = |M_{i+j-1}| \geq |\Lambda_i - \Lambda_j| \geq \min\{\lambda_i + \lambda_j - 1, p\} \tag{6}$$

for $1 \leq i, j \leq m$.

Therefore, the conditions of Lemma 4 are satisfied, so

$$|A - A| = \sum_{k=1}^{p} \mu_k \geq (2n+1)p$$

as desired. $\square$

7. Completing the proof of Theorem 5

Before proceeding to the proof of Theorem 5, we prove a general lemma about sets in vector spaces over finite fields.

Lemma 5. *Let p be a prime and let m be an integer. Let G be a vector space over the field $\mathbb{F}_p$ of dimension $d \geq 3$, and let S be a subset of G such that*

$$|S \cap H| \geq mp^{d-2}$$

for each vector hyperplane H (that is, vector subspace of dimension $d-1$) in G. Then $|S| \geq mp^{d-1}$.

Proof of Lemma 5. Assume for the sake of contradiction that $|S| < mp^{d-1}$. We first claim that there is a $(d-2)$-dimensional vector subspace $V_0 \subset G$ with $|S \cap V_0| \leq mp^{d-3}$. To show this, take a $(d-2)$-dimensional vector subspace $V \subset G$ uniformly at random. It is clear that V has $p^{d-2} - 1$ nonzero elements, that G has $p^d - 1$ nonzero elements, and that each nonzero element of G is in V with equal probability. Therefore, the probability that $x \in V$ for a fixed $x \in G \setminus \{0\}$ is

$$\frac{p^{d-2} - 1}{p^d - 1}.$$

Clearly, the probability that $0 \in V$ is 1. Therefore, by the linearity of expectation, the expected value of $|S \cap V|$ is given by

$$\begin{aligned}\mathbb{E}[|S \cap V|] &= 1 + (|S| - 1)\frac{p^{d-2} - 1}{p^d - 1} \\ &< 1 + (mp^{d-1} - 1)\frac{p^{d-2} - 1}{p^d - 1} \\ &= mp^{d-3} + \frac{(p^2 - 1)(p - m)p^{d-3}}{p^d - 1} \\ &< mp^{d-3} + 1.\end{aligned}$$

Since mp^{d-3} is an integer, we conclude that there is a particular $(d-2)$-dimensional vector subspace $V_0 \subset G$ with $|S \cap V_0| \leq mp^{d-3}$.

Finally, consider the integer N defined by the sum

$$N = \sum_H |S \cap H|$$

where H ranges over all vector hyperplanes with $V_0 \subset H \subset G$. Such hyperplanes H are in bijection with lines through the origin in the two-dimensional quotient space G/V_0, so there are $p+1$ of them. Therefore, by the assumption of the theorem, we have

$$N \geq \sum_H mp^{d-2} = (p + 1)mp^{d-2}.$$

On the other hand, the sum defining N counts every element of $S \setminus V_0$ once and every element of $S \cap V_0$ exactly $p + 1$ times, so

$$N = |S| + p|S \cap V_0|.$$

Therefore, we have

$$|S| = N - p|S \cap V_0| \geq (p + 1)mp^{d-2} - p \cdot mp^{d-3} = mp^{d-1},$$

which contradicts our assumption that $|S| < mp^{d-1}$. □

We are now ready to restate and prove Theorem 5.

Theorem 5. *Let $G = (\mathbb{Z}/p\mathbb{Z})^d$ where p is prime and $d \geq 0$. Let t and r be integers with $0 \leq t \leq d$ and $p^t < r \leq p^{t+1}$. Then*

$$\rho_G^-(r) = p^t \min\left\{2\left\lceil \frac{r}{p^t} \right\rceil - 1, p\right\}.$$

Proof. We proceed by induction on r. If $t < 2$, then the result follows from Lemma 3, so we may assume $t \geq 2$. By Lemma 2, we may also assume that $d = t+1$. Let $m = \min\{2\lceil r/p^t \rceil - 1, p\}$. We wish to show that $\rho_G^-(r) = mp^t$. By Lemma 1, we have $\rho_G^-(r) \leq mp^t$, so it remains

to show that $\rho_G^-(r) \geq mp^t$. Let A be a subset of G with $|A| = r$; we will show that $|A - A| \geq mp^t$.

Consider G as a vector space of dimension $d = t+1 \geq 3$ over $\mathbb{F}_p$. By Lemma 5 applied to $S = A-A$, it suffices to show that $|(A-A)\cap H| \geq mp^{t-1}$ for each vector hyperplane $H \subset G$. For this, note that there are exactly p distinct translates $H + x$, where $x \in G$, and that the entire space G is the disjoint union of these p translates. Therefore, there exists $x_0 \in G$ such that $|A \cap (H + x_0)| \geq \lceil r/p \rceil$. By the inductive hypothesis,

$$|(A-A)\cap H| \geq |(A\cap(H+x_0))-(A\cap(H+x_0))| \geq \rho_H^-(\lceil r/p\rceil) = mp^{t-1}$$

as desired. □

8. Applications to signed sumsets

In this section, we prove Theorem 6. In particular, we will show that it is a consequence of the following more general result. The notations $\rho_\pm(G, m, r)$ and $r_\pm A$ used in this section are defined in [2].

Lemma 6. *Let G be a finite abelian group of order N. Then*

$$\rho_\pm(G, m, 2) \geq \min\{\rho_G^-(m), \rho_G^-(2m) - 1\}$$

for $1 \leq m \leq N/2$.

Proof. Let $A \subseteq G$ be a subset with $|A| = m$. We will show that

$$2_\pm A \geq \min\{\rho_G^-(m), \rho_G^-(2m) - 1\}.$$

We consider two cases, depending on whether or not $A \cap (-A) = \emptyset$.

Case 1 ($A \cap (-A) \neq \emptyset$)**:**
Choose $x \in A \cap (-A)$. By definition, the signed sumset $2_\pm A$ contains $0 = x+(-x)$ and it contains the difference of any two distinct elements of A. Therefore, we have $A - A \subseteq 2_\pm A$. It follows that

$$|2_\pm A| \geq |A - A| \geq \rho_G^-(m) \geq \min\{\rho_G^-(m), \rho_G^-(2m) - 1\},$$

as desired.

Case 2 ($A \cap (-A) = \emptyset$)**:**
Let $B = A \cup (-A)$. Then $|B| = 2|A|$. By definition, the signed sumset $2_\pm A$ contains $(B - B) \setminus \{0\}$, so

$$\begin{aligned} |2_\pm A| &\geq |B - B| - 1 \\ &\geq \rho_G^-(2m) - 1 \\ &\geq \min\{\rho_G^-(m), \rho_G^-(2m) - 1\}, \end{aligned}$$

as desired. □

Now, we shall restate and prove Theorem 6.

Theorem 6 ([2, Conjecture 18])**.** *Let $p > 2$ be a prime number, and let c and v be integers with $0 \le c \le p-1$ and $1 \le v \le p$. Let $m = cp+v$.*
(a) If $1 \le c \le (p-3)/2$, then

$$\rho_{\pm}((\mathbb{Z}/p\mathbb{Z})^2, m, 2) = (2c+1)p.$$

(b) If $c = (p-1)/2$ and $v \le (p-1)/2$, then

$$\rho_{\pm}((\mathbb{Z}/p\mathbb{Z})^2, m, 2) = p^2-1.$$

Proof. (a) By Lemma 6 and Theorem 5, we have

$$\begin{aligned}\rho_{\pm}((\mathbb{Z}/p\mathbb{Z})^2, m, 2) &\ge \min\{\rho^-_G(m), \rho^-_G(2m)-1\}\\ &= \min\left\{(2c+1)p, \left(4c+2\left\lceil\frac{2v}{p}\right\rceil+1\right)p-1\right\}\\ &= (2c+1)p.\end{aligned}$$

The reverse inequality $\rho_{\pm}((\mathbb{Z}/p\mathbb{Z})^2, m, 2) \le (2c+1)p$ follows from [1, Theorem 5].

(b) By Lemma 6 and Theorem 5, we have

$$\begin{aligned}\rho_{\pm}((\mathbb{Z}/p\mathbb{Z})^2, m, 2) &\ge \min\{\rho^-_G(m), \rho^-_G(2m)-1\}\\ &= \min\{p^2, p^2-1\}\\ &= p^2-1.\end{aligned}$$

The reverse inequality $\rho_{\pm}((\mathbb{Z}/p\mathbb{Z})^2, m, 2) \le p^2-1$ follows from [1, Proposition 8].

□

A. Proof of Lemma 4

In this appendix, we prove Lemma 4. The following lemma is essential to our proof of Lemma 4.

Lemma A.1. *Let $m > 1$, and let $\lambda = (\lambda_1, \dots, \lambda_m)$ be a sequence of integers with $\lambda_1 \ge \cdots \ge \lambda_m > 0$ and $\lambda_1 > 1$. Define the sequence $\mu = (\mu_1, \dots, \mu_{2m-1})$ by*

$$\mu_k = \max_{k=i+j-1}(\lambda_i + \lambda_j - 1)$$

for $1 \le k \le 2m-1$, where the maximum is over all $1 \le i, j \le m$ with $k = i+j-1$. Then

$$\sum_{k=1}^{2m-1} \mu_k \ge 3\left(\sum_{k=1}^{m} \lambda_k\right) - 3.$$

Proof. Let

$$F(\lambda) = \{(x, y) \in \mathbb{Z}^2 \mid 0 \le y \le m-1, 0 \le x \le \lambda_{y+1} - 1\} \subset \mathbb{Z}^2$$

be the Ferrers diagram of λ; that is, a set with m rows of points where the kth row from the bottom contains λ_k points for $1 \le k \le m$. Similarly, let

$$F(\mu) = \{(x, y) \in \mathbb{Z}^2 \mid 0 \le y \le 2m-2, 0 \le x \le \mu_{y+1} - 1\} \subset \mathbb{Z}^2$$

be the Ferrers diagram of μ.

We claim that $F(\mu)$ contains the sumset $F(\lambda) + F(\lambda)$. To show this, take two elements (x, y) and (x', y') in $F(\lambda)$; we wish to show that $(x + x', y + y') \in F(\mu)$. By the definition of $F(\lambda)$ we have

$$\begin{aligned} 0 &\le y + y' \le (m-1) + (m-1) = 2m-2 \\ 0 &\le x + x' \le (\lambda_{y+1} - 1) + (\lambda_{y'+1} - 1) \le \mu_{y+y'+1} - 1 \end{aligned}$$

so $(x + x', y + y') \in F(\mu)$ as desired.

By assumption, both $m > 1$ and $\lambda_1 > 1$, so $F(\lambda)$ contains the three non-collinear points $(0, 0)$, $(1, 0)$, and $(0, 1)$. Therefore, by Freiman's dimension lemma [12, Theorem 5.20],

$$\sum_{k=1}^{2m-1} \mu_k = |F(\mu)| \ge |F(\lambda) + F(\lambda)| \ge 3|F(\lambda)| - 3 = 3\left(\sum_{k=1}^{m} \lambda_k\right) - 3$$

as desired. □

We shall now restate and prove Lemma 4.

Lemma 4. *Let p be a prime, and let m and n be integers with $n \ge 1$ and $n + 2 \le m \le (p-1)/2$. Let $\lambda = (\lambda_1, \ldots, \lambda_m)$ be a sequence of integers with $p \ge \lambda_1 \ge \cdots \ge \lambda_m > 0$ and $\sum_{k=1}^{m} \lambda_k \ge np + 1$. Let $\mu = (\mu_1, \ldots, \mu_{2m-1})$ be a sequence of integers such that $\mu_{i+j-1} \ge \min\{\lambda_i + \lambda_j - 1, p\}$ for $1 \le i, j \le m$. Then*

$$\sum_{k=1}^{2m-1} \mu_k \ge (2n+1)p.$$

Proof of Lemma 4. We may assume that

$$\mu_k = \max_{k=i+j-1} \min\{\lambda_i + \lambda_j - 1, p\}$$

for all k. Let h be the maximum value of $i + j - 1$ over all integers $1 \le i, j \le m$ with $\lambda_i + \lambda_j - 1 > p$, or 0 if no such i and j exist. Then $\mu_k = p$ for $k \le h$ and $\mu_{i+j-1} \ge \lambda_i + \lambda_j - 1$ for $1 \le i, j \le m$ as long as $i + j - 1 > h$.

Proceed by induction on m. We consider three cases, depending on whether $h = 0$ or $h = 1$ or $h \ge 2$.

Case 1 ($h = 0$)**:**
Then Lemma A.1 applies, so

$$\begin{aligned}\sum_{k=1}^{2m-1} \mu_k &\geq 3\left(\sum_{k=1}^{m} \lambda_k\right) - 3 \\ &\geq 3(np+1) - 3 \\ &\geq (2n+1)p\end{aligned}$$

as desired.

Case 2 ($h = 1$)**:**
First assume $n = 1$ and $m = 3$. Then

$$\begin{aligned}\sum_{k=1}^{2m-1} \mu_k &= \mu_1 + \mu_2 + \mu_3 + \mu_4 + \mu_5 \\ &\geq p + (\lambda_1 + \lambda_2 - 1) + (\lambda_1 + \lambda_3 - 1) + (\lambda_2 + \lambda_3 - 1) + 1 \\ &\geq p + 2(\lambda_1 + \lambda_2 + \lambda_3) - 2 \\ &\geq p + 2(p+1) - 2 \\ &= 3p\end{aligned}$$

as desired.

Next assume $n = 1$ and $m \geq 4$. The assumption that $h = 1$ implies that $2\lambda_1 - 1 > p$, so $\lambda_1 > (p+1)/2$. Therefore $\mu_k \geq \lambda_1 + \lambda_k - 1 > (p+1)/2$ for $1 < k < m$ and $\mu_k \geq \lambda_m + \lambda_{k-m+1} - 1 \geq \lambda_{k-m+1}$ for $k \geq m$, so

$$\begin{aligned}\sum_{k=1}^{2m-1} \mu_k &> p + \sum_{k=2}^{m-1} \frac{p+1}{2} + \sum_{k=m}^{2m-1} \lambda_{k-m+1} \\ &= p + (m-2)\frac{p+1}{2} + (np+1) \\ &> 3p\end{aligned}$$

as desired.

It remains to consider the case that $n \geq 2$. Because $h = 1$, Lemma A.1 applies to the sequences $(\lambda_1, \cdots, \lambda_m)$ and $(2p-1, \mu_2, \cdots, \mu_{2m-1})$. Therefore

$$\begin{aligned}\sum_{k=1}^{2m-1} \mu_k = p + \sum_{k=2}^{2m-1} \mu_k \\ &= -p + 1 + \left(2p - 1 + \sum_{k=2}^{2m-1} \mu_k\right) \\ &\geq -p + 1 + 3(np+1) - 3 \\ &\geq (2n+1)p\end{aligned}$$

as desired.

Case 3 $(h \geq 2)$**:**
Define the sequence $\lambda' = (\lambda'_1, \ldots, \lambda'_{m-1})$ by $\lambda'_k = \lambda_{k+1}$ for $1 \leq k \leq m-1$. Then, define $\mu' = (\mu'_1, \ldots, \mu'_{2m-3})$ by

$$\mu'_k = \max_{k=i+j-1} \min\{\lambda'_i + \lambda'_j - 1, p\}$$

for $1 \leq k \leq 2m-3$, where the maximum is over all $1 \leq i, j \leq m-1$ with $k = i + j - 1$. We have

$$\sum_{k=1}^{m-1} \lambda'_k = \left(\sum_{k=1}^{m} \lambda_k\right) - \lambda_1 \geq (n-1)p + 1,$$

so by the inductive hypothesis we have

$$\sum_{k=1}^{2m-3} \mu'_k \geq (2n-1)p.$$

On the other hand, we have

$$\mu_{k+2} = \max_{k+2=i+j-1} (\lambda_i + \lambda_j - 1) \geq \max_{k=i+j-1} (\lambda'_i + \lambda'_j - 1) = \mu'_k$$

for $1 \leq k \leq 2m-3$, where the inequality follows from replacing (i, j) with $(i-1, j-1)$. Therefore

$$\sum_{k=1}^{2m-1} \mu_k = 2p + \sum_{k=1}^{2m-3} \mu'_k \geq (2n+1)p$$

as desired. $\square$

Acknowledgments

This research was conducted under the supervision of Joseph Gallian at the University of Minnesota Duluth REU, funded by NSF Grant 1358659 and NSA Grant H98230-13-1-0273. The author thanks Joseph Gallian, who ran the REU, brought this question to his attention, and provided helpful comments on the manuscript. He thanks his advisors Levent Alpoge and Benjamin Gunby for valuable discussions and advice.

References

[1] Béla Bajnok and Ryan Matzke. The minimum size of signed sumsets. *Electr. J. Comb.*, 22(2):P2.50, 2015.

[2] Béla Bajnok and Ryan Matzke. On the minimum size of signed sumsets in elementary abelian groups. *Journal of Number Theory*, 159:384 – 401, 2016.

[3] Boris Bukh. Sums of dilates. *Combinatorics, Probability and Computing*, 17(05):627–639, 2008.

[4] Augustin-Louis Cauchy. Recherches sur les nombres. In *Oeuvres complètes*, volume 1, pages 39–63. Cambridge University Press, 2009. Cambridge Books Online.

[5] Harold Davenport. On the addition of residue classes. *Journal of the London Mathematical Society*, 1(1):30–32, 1935.

[6] Shalom Eliahou and Michel Kervaire. Sumsets in vector spaces over finite fields. *J. Number Theory*, 71(1):12–39, 1998.

[7] Shalom Eliahou and Michel Kervaire. Minimal sumsets in infinite abelian groups. *Journal of Algebra*, 287(2):449 – 457, 2005.

[8] Martin Kneser. Abschätzung der asymptotischen dichte von summenmengen. *Mathematische Zeitschrift*, 58(1):459–484, 1953.

[9] Alain Plagne. Optimally small sumsets in groups. I. The supersmall sumsets property, the $\mu_G^{(k)}$ and the $\nu_G^{(k)}$ functions. *Unif. Distrib. Theory*, 1(1):27–44, 2006.

[10] Alain Plagne. Sums of dilates in groups of prime order. *Combinatorics, Probability and Computing*, 20(06):867–873, 2011.

[11] Gonzalo Fiz Pontiveros. Sums of dilates in $\mathbb{Z}_p$. *Combinatorics, Probability and Computing*, 22(02):282–293, 2013.

[12] Terence Tao and Van H Vu. *Additive combinatorics*, volume 105. Cambridge University Press, 2006.

Harvard University
E-mail address: `mitchell@math.harvard.edu`